LEGISLATIVE LIBRARY OF BRITISH COLUMBIA
3 3298 00313 5838

# OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER

*for*

*British Columbia*

## 2005–2006 ANNUAL REPORT

DOC
BC
I4606
B
2005/06
c.3

106-06989/

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
*for*
*British Columbia*

# 2005-2006 ANNUAL REPORT

**Library and Archives Canada Cataloguing in Publication Data**

British Columbia. Office of the Information and Privacy Commissioner. Annual report (CD-ROM)

Annual report [electronic resource]. –2005/2006–

Annual

CD-ROM format.

Issued also in printed form on demand.

Report year ends Mar. 31.

ISSN 1911-0278 = Annual report (British Columbia. Office of the Information & Privacy Commissioner. CD-ROM)

1. British Columbia. Office of the Information and Privacy Commissioner – Periodicals. 2. British Columbia. Freedom of Information and Protection of Privacy Act. 3. Privacy, Right of – British Columbia – Periodicals. 4. Government information – British Columbia – Periodicals. 5. Public records – British Columbia – Periodicals. I. British Columbia. Office of the Information and Privacy Commissioner. II. Title.

KEB505.62 342.711'062 C2006-960094-5

KF5753.I5B74

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

June 30, 2006

Hon. Bill Barisoff
Speaker of the Legislative Assembly
Legislative Assembly of British Columbia
Victoria, BC V8V 1X4

Dear Speaker Barisoff:

Under section 51 of the *Freedom of Information and Protection of Privacy Act* and section 44 of the *Personal Information Protection Act*, I have the honour to present the Office's twelfth Annual Report to the Legislative Assembly.

This report covers the period from April 1, 2005 to March 31, 2006.

Yours sincerely,

**David Loukidelis**
Information and Privacy Commissioner
for British Columbia

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Third Floor, 756 Fort Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through Enquiry BC at (800) 663-7867 or (604) 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

# TABLE OF CONTENTS


**1 COMMISSIONER'S MESSAGE** 1

The Challenge of Handling an Increasing Demand for Our Services ..... 1
Privacy Breaches ..... 2
PIPA Awareness ..... 2
New Information Technology Challenges ..... 3
Improving BC's Information and Privacy Legislation ..... 3
Statistical Snapshot: Total OIPC Files, 2005-06 ..... 4

**2 CRITICAL ISSUE: PRIVACY BREACHES** 5

Breach Notifications in 2005-06 ..... 5
Safeguards to Prevent Breaches ..... 5
Four Key Steps in Responding to Privacy Breaches ..... 7

**3 THE YEAR IN REVIEW: FIPPA FILES** 9

Requests for Review: Resolving Disputes through Mediation ..... 9
Case Summaries: Requests for Review ..... 12
Investigating and Resolving FIPPA Access Complaints ..... 17
Case Summaries: FIPPA Access Complaints ..... 18
Investigating and Resolving FIPPA Privacy Complaints ..... 19
Case Summaries: FIPPA Privacy Complaints ..... 21
Orders and Other Decisions ..... 25
Case Summaries: FIPPA Orders ..... 26

**4 THE YEAR IN REVIEW: PIPA FILES** 30

Investigating and Resolving PIPA Requests for Review and Complaints ..... 30
Case Summaries: PIPA Complaints ..... 32
Case Summaries: PIPA Requests for Review ..... 38
Case Summaries: PIPA Orders ..... 40

**5 THE YEAR IN REVIEW: OTHER OIPC ACTIVITIES** 42

Comments on Proposed Policy and/or Program Initiatives ..... 42
Public Information Initiatives ..... 43

**ORGANIZATIONAL CHART** 45

**FINANCIAL REPORTING** 46

## LIST OF TABLES

Table 1. Total FIPPA and PIPA Files Received and Closed ..... 4
Table 2. Disposition of FIPPA Requests for Review, by Type ..... 10
Table 3. Disposition of FIPPA Requests for Review, by Public Body ..... 11
Table 4. Disposition of FIPPA Access Complaints, by Type ..... 18
Table 5. Disposition of FIPPA Privacy Complaints, by Type ..... 20
Table 6. Types of FIPPA Access and Privacy Complaints, by Public Body ..... 21
Table 7. Disposition of PIPA Complaints, by Type ..... 31
Table 8. Disposition of PIPA Requests for Review, by Type ..... 32

# 1 COMMISSIONER'S MESSAGE

Thinking it would be my last, I used last year's annual report message as an opportunity to look back on my term as Information and Privacy Commissioner. This first message of my second six-year term in the position allows me to look forward at the next several years in access and privacy.

Let me first say how grateful I am to have been re-appointed last November on the unanimous recommendation of the Legislative Assembly. It has been, and continues to be, a great privilege to serve the public in the areas of access to information and privacy protection. I will serve to the best of my abilities, with energy and diligence.

This year we are presenting the office's annual report in a new format with new features. We are distributing the report on a CD and are placing additional resources on the CD. The portions of past annual reports describing the role and mandate of the office, as well as questions and answers about privacy in the hiring process, are included on the CD. In addition, links to full documents on our website are included where the document is mentioned in the report.

## The Challenge of Handling an Increasing Demand for Our Services

Before taking a look at what's ahead, I should review the past year. During the year ended March 31, 2006, we closed 5,504 files, another record for our office. These files cover the wide range of activities in which our office engages, including requests for review (access to information appeal mediations and adjudications); extensions of time for public bodies to respond to access requests; applications to disregard access to information requests; privacy breach notifications; privacy complaints; access requests to our office as a public body under the legislation; reviews of proposed legislation; policy consultations by public bodies; privacy impact assessment reviews; requests for information about the legislation and other matters; speaking engagements; and media interviews.

In last year's annual report, I expressed concern about our funding and whether it was sufficient to allow us to do our job in a timely and professional fashion. During the last fiscal year, our office received, with the support of a committee of the Legislative Assembly, a 10% increase in the budget for fiscal 2006-07. This increase, which flowed from a request that I made to the Committee last December, is intended to help us deal with increasing demands for our services in both the public and private sectors. That funding is in the process of being invested now in staffing for the office and to enable us to more proactively assist public and private sector organizations with their privacy compliance responsibilities and, in the public sector, access to information duties.

As I said in last year's message, an effective access and privacy law requires effective oversight of compliance, which in turn depends on adequate funding for the oversight agency. I expressed concern last year that we were not properly discharging our duties to the public and that we needed more resources to deal with increased workloads. In light of the 10% increase in funding that has been given to us for fiscal 2006-07, I will continue to monitor the situation as we move forward.

## Privacy Breaches

In early March, in the first of several privacy breaches that came to light that month, it was reported that the provincial government had sold 41 used computer backup tapes at a public auction. The tapes contained sensitive personal information of thousands of British Columbia residents. The tapes' purchaser took them to *The Vancouver Sun*, which published several stories at the beginning of March. We quickly investigated and, in our report on the investigation,[1] faulted the provincial government for not having taken reasonable security measures to protect the personal information against unauthorized disclosure.

Other disclosures of personal information by public sector bodies came to light in March, as did some disclosures by private sector organizations. These are still under investigation, but they highlight a problem that has had a good deal of publicity in British Columbia and elsewhere. Because I am concerned about disclosures of personal information due to inadequate security measures in the public and private sectors, I have asked my colleagues in the office to come up with a variety of resources to address the problem. A special section of this report describes the issues and the steps we are taking to help private sector and public sector organizations to protect the personal information with which they are entrusted.

## PIPA Awareness

The steady increase in the number of PIPA complaints and requests for review this year reflects steadily growing public concern about personal information protection. I released my first PIPA order discussing the collection of personal information when a customer returns goods to a large retailer. A summary of this case is found later in this report.

In response to feedback received last year during our public consultation on PIPA and employment issues, this office has recently released a question and answer document entitled "PIPA and the Hiring Process".[2] This piece assists employers and employees (or potential employees) in the collection and use of personal information at the time of hire. I am considering expanding this document to cover a wider range of issues.

[1] *Sale of Provincial Government Computer Tapes Containing Personal Information*, Investigation Report F06-01 (March 31, 2006). http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf.

[2] http://www.oipc.bc.ca/pdfs/private/PIPAHiringFAQ(10APR06).pdf.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

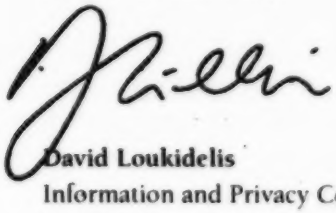
## New Information Technology Challenges

We will also continue our work this year in monitoring the risks and rewards that information technologies offer for privacy, in both the public and private sectors. In last year's message, I expressed concern about the impact of information technology on privacy in the context of national security and anti-terrorism. We will continue to watch carefully as information technologies develop and are deployed in the name of national security.

In the private sector, there are signs that radio frequency identification (RFID) technologies are on the verge of rollout in the business-to-business context – notably in supply chain management – though not yet in the business-to-consumer context. But because of the power of RFID, and its likely rollout at some point in the B2C (business-to-consumer) context, our office is working on a discussion document and guidance on RFID and privacy. I do not favour special legislation to address privacy implications of RFID, since existing Canadian privacy laws are, in my view, adequate to the task. Still, I believe guidance would be of use to businesses as they contemplate using RFID in B2C applications. We will continue to work in this area, in co-operation with colleagues elsewhere in Canada, and will publish the document in the current fiscal year.

## Improving BC's Information and Privacy Legislation

Again looking forward, I am concerned that the unanimous recommendations of the Special Committee to Review the Freedom of Information and Protection of Privacy Act, released in May of 2004, were not acted upon by fiscal year-end. As I emphasized in last year's annual report (pp. 10-11), it is important that these recommendations be implemented in order to buttress and enhance the public's right of access to information and to help my office do its work more efficiently and effectively. I will continue to work with government officials to encourage implementation of these recommendations without delay.



**David Loukidelis**
Information and Privacy Commissioner for British Columbia
June 2006

## Statistical Snapshot: Total OIPC Files, 2005-06

Table 1 provides an overview of our work in 2005-06, categorized by the number of files we dealt with in each area of activity.

TABLE 1 TOTAL FIPPA AND PIPA FILES RECEIVED AND CLOSED, 1 APR 05 - 31 MAR 06

| | DISPOSITION | |
|---|---|---|
| **FILE TYPE** | **FILES RECEIVED** | **FILES CLOSED** |
| General requests for information | 3694 | 3694 |
| Requests for review of decisions to withhold information by public bodies or organizations | 611 | 615 |
| Complaints whether public bodies or organizations have carried out their responsibilities under FIPPA or PIPA | 475 | 508 |
| Policy or issue consultations requested by public bodies or organizations | 161 | 188 |
| Requests by public bodies or organizations for a time extension to respond to requests for records | 79 | 79 |
| Queries to OIPC from the media | 68 | 68 |
| Speaking engagements by OIPC staff | 68 | 68 |
| Meetings with public bodies or organizations | 43 | 43 |
| Reviews of legislative changes that may affect privacy or access to information | 40 | 37 |
| Notifications of privacy breaches by public bodies or organizations | 34 | 23 |
| Research and policy development | 29 | 29 |
| Requests by applicants for a time extension to request a review of a decision | 27 | 27 |
| Issues where our office does not have jurisdiction over a public body or organization (e.g., federal agencies, banks) | 26 | 26 |
| Issues where our office has jurisdiction but there is no issue that our office can review | 23 | 23 |
| Conference attendance by OIPC staff | 20 | 20 |
| Investigations into access to information or privacy issues | 17 | 14 |
| Public notifications under s. 25 (e.g., health issues, dangerous offenders) | 10 | 10 |
| Other | 10 | 8 |
| Freedom of information requests to OIPC | 9 | 9 |
| Site visits by the Commissioner to public bodies or organizations | 6 | 6 |
| Reconsiderations of mediation outcomes | 6 | 6 |
| Reviews of privacy impact assessments developed by public bodies or organizations | 3 | 2 |
| Application by public bodies or organizations to disregard requests by an applicant considered vexatious or repetitious | 2 | 2 |
| **Total** | **5432** | **5504** |

# 2 CRITICAL ISSUES: PRIVACY BREACHES

In order to meet their obligations under the *Freedom of Information and Protection of Privacy Act* (FIPPA) or the *Personal Information Protection Act* (PIPA), public bodies and organizations must take steps to protect themselves against privacy breaches and to react appropriately should a privacy breach occur. The following discussion includes a definition of a "privacy breach", examples of the types of privacy breaches reported to the OIPC in the past year, suggestions for preventing a privacy breach and, finally, four key steps public bodies and organizations should take if a privacy breach occurs.

A privacy breach occurs when there is unauthorized collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of PIPA or Part 3 of FIPPA. The most common privacy breach happens when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed.

## Breach Notifications in 2005-06

Of the 34 breach notifications received by the OIPC in 2005-06, 22 were related to FIPPA and 12 to PIPA.

The most common privacy breach that occurred was as a result of theft. Thieves stole everything from computers to backpacks, bins of paper set out for shredding to vials of HIV positive blood. In every case, the public body or organization had failed to properly secure the personal information to prevent access in the event of theft. A second common example of a privacy breach was loss of records by courier companies. In one case, the driver left the vehicle running and unlocked during a delivery. The vehicle was stolen with medical files in it. Less common, but still persistent, were reports of misuse of personal information by employees. Generally, the cases involved accessing data base information regarding a particular third party for non-work related purposes.

Perhaps the most high profile types of privacy breaches are those related to inappropriate disposal – the cases of medical and legal files blowing down the street or the case of the sale of government computers with personal information still contained on the hard drives.

## Safeguards to Prevent Breaches

Public bodies and organizations can use a number of safeguards to protect against privacy breaches. As a result of our investigations into the privacy breaches reported

this year, we have developed the following list of suggested safeguards that may assist in reducing the chances of a privacy breach.

**(a) Theft of computers and other media**

Criminal activity is a risk that must be considered when assessing whether security arrangements are reasonable. Consider the following safeguards:

- Appoint a security officer and develop and implement a security plan.
- Increase the number of barriers that will deter, if not stop, a thief, such as alarms, lighting and computer bolts.
- Store personal information on an on-site network server in a secure location.
- Password protect and encrypt[3] sensitive personal information.
- Keep laptop computers under your control at all times. Lock laptops in a secure place after working on them at home.

**(b) Faxing and emailing personal information**

You should not fax or email sensitive personal information unless speed of transmission is essential. If faxing or emailing is the only timely method available, extra precautions are required. Consider the following safeguards:

- Set rules about the types of personal information that can be faxed or emailed to or from your organization.
- Locate your fax machine in a secure area and monitor sensitive faxes.
- Phone ahead to confirm the fax number or email address before sending personal information.
- Use encryption technology to email or fax sensitive personal information.
- Never use an email distribution list to send sensitive personal information.

**(c) Transporting records by courier**

You should always use a reputable courier company and consider the following additional safeguards:

- Ensure the courier company has adequate security measures to protect personal information, including physical security and bonded employees.
- Ensure the courier company tracks the shipment and collects the signature of the receiver when the delivery is made.
- Call the receiver of sensitive information to confirm pick-up and ask it to confirm receipt of the records.

**(d) Destruction of records**

Public bodies and organizations should establish clear records-destruction policies.

[3] Encryption is a method to obscure information so that it is unreadable by anyone but those who are intended to read or receive the information. The use of a password to protect sensitive personal information will not, by itself, meet the test of reasonable security measures.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

Procedures that ensure confidentiality is maintained should be used when documents are destroyed. Destroy records in a way that prevents the information in the records from being retrieved or reconstructed. Consider the following safeguards:

- In-house, cross-cut shredding is the most secure method to destroy sensitive paper records. If you use off-site shredding services, use only reputable services with experience destroying sensitive records. Ensure that the shredding service has adequate security measures.
- Simply deleting computer files or reformatting a disk does not securely destroy the data. The secure way to destroy data is by physical destruction of the disk or hard drive or by "wiping". Wiping is the process of writing and re-writing blank data over the disk until all traces of the original data are destroyed. Specialized software is required to securely wipe a disk.

## Four Key Steps in Responding to Privacy Breaches

Public bodies and organizations must respond at once to a privacy breach. Rapid action by public bodies and organizations after a privacy breach is part of their responsibility for protection of personal information. The steps are:

1. Contain the breach
2. Evaluate the risks associated with the breach
3. Notify affected parties as necessary
4. Prevent future breaches

### Step 1: Contain the breach

- Immediately contain the breach by seeking return of the records, shutting down the system that was breached, correcting weaknesses in physical security, etc.
- Immediately contact your Director/Manager of Information and Privacy, privacy officer or security officer.
- Notify the police if the breach involves theft or other criminal activity.

### Step 2: Evaluate the risks associated with the breach

To determine what further steps are immediately necessary, first assess the risks associated with the breach, considering the following factors:

- What kinds of personal information are involved?
- What is the cause of the breach? Is there a risk of further exposure?
- How many individuals are affected by the breach?
- Is the information encrypted or otherwise not easily exploited?
- What harm to individuals might result from the breach (including risk to public health, identity theft, loss of business or employment opportunities, hurt, humiliation, damage to reputation or relationships)?
- What harm might your organization suffer due to the breach?

**Step 3: Notify affected parties as necessary**

The key consideration is whether you should notify affected individuals of the breach to avoid or mitigate harm to them. You should review the risk assessment under Step 2 to assess whether notification is required and to address the following notification considerations.

There are four groups of individuals that may require notification:

- Individuals whose personal information is involved in the breach
- Other organizations that may be affected by the breach
- Other groups may require notice based on legal, professional or contractual obligations
- The Office of the Information and Privacy Commissioner for British Columbia (OIPC).[4]

You can notify affected individuals directly or by a substitute method. Choose the method that will most effectively mitigate the harm you have identified.

Notifications should include the following pieces of information:

- The fact that a privacy breach occurred and a description of it.
- The elements of personal information involved.
- The steps you have taken to mitigate the harm and any likely further steps.
- Advice to affected individuals on what they can do to further mitigate the risk of harm.
- The fact that affected individuals have a right to complain to the OIPC.

**Step 4: Prevent Future Breaches**

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach (including through a security audit of both physical and technical security). Use the audit results to develop adequate long-term safeguards to prevent further breaches. You should review and update your policies to reflect the lessons learned and should refresh staff training on privacy obligations under British Columbia's applicable privacy law.

[4] The following factors are relevant in deciding when to report a breach to the OIPC: the sensitivity of the personal information; whether the disclosed information could be used to commit identity theft; whether there is a reasonable chance of harm from the disclosure, including non-pecuniary losses; the number of people affected by the breach; and whether the information was fully recovered without further disclosure.

# 3 THE YEAR IN REVIEW: FIPPA FILES

## Requests for Review: Resolving Disputes through Mediation

When a public body decides to sever or withhold information in response to an application for access, the *Freedom of Information and Protection of Privacy Act* (FIPPA) gives the applicant the right to ask us to review that decision. An applicant wishing to request a review must do so within 30 business days after receiving a public body's response to the access request and must include a copy of the original response and the public body's written decision.

Section 55 of FIPPA allows the Commissioner to authorize mediation for any matter under review. It is the normal practice for the OIPC to refer a review to a Portfolio Officer, who will try to resolve the matter through mediation. In this process, the Portfolio Officer is not an advocate for either side. Mediation fosters ongoing discussion between the requester and the public body and is less expensive, less onerous and more expedient than a formal inquiry.

In attempting to mediate reviews, the Portfolio Officer ensures the applicant has received all of the information he or she is entitled to receive. This typically involves discussing the issue with all parties; reviewing the records in dispute; examining the legislation; considering previous relevant decisions by the OIPC, other commissioners and the courts; and attempting to generate mutually acceptable options for resolution of the matter. FIPPA allows 90 business days to resolve a review. If the matter cannot be resolved during this time, the matter may proceed to a formal inquiry before the Commissioner or his delegate.

Mediation of reviews may result in a number of outcomes, including the following:

- More information is released.
- The issues in dispute are narrowed.
- The public body's decision is further clarified.
- The applicant's initial request is further clarified.
- The matter is referred to another agency for resolution.
- An applicant's questions or concerns underlying the request are addressed.

In fiscal 2005-06, our office received 559 requests for review under FIPPA (see Table 2). Of the 566 requests for review we closed during this period, 56 resulted in a notice of inquiry being issued.

TABLE 2. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY TYPE

| | DISPOSITION | | | | | | |
|---|---|---|---|---|---|---|---|
| PUBLIC BODY | MEDIATED | NO REVIEWABLE ISSUE | NON JURISDICTIONAL | REFERRED TO PUBLIC BODY | WITHDRAWN | NOTICE OF INQUIRY ISSUED | TOTAL |
| Some information withheld from applicant (ss.12-22.1) | 240 | 6 | 1 | 2 | 43 | 29 | 321 |
| Failure to respond within required timelines (s.7) | 76 | 15 | 0 | 5 | 12 | 4 | 112 |
| All information withheld from applicant (ss.12-22.1) | 70 | 3 | 3 | 2 | 9 | 20 | 107 |
| Requested records not covered by FIPPA (ss.3&4) | 8 | 0 | 1 | 0 | 2 | 1 | 12 |
| Third party objects to disclosure of their information (s.24) | 5 | 1 | 0 | 0 | 0 | 2 | 8 |
| Conflict between FIPPA and other legislation (s.79) | 5 | 0 | 0 | 0 | 0 | 0 | 5 |
| Refusal to confirm or deny the existence of records (s.8) | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| **Total** | **405** | **25** | **5** | **9** | **66** | **56** | **566** |

In any given year, public bodies that handle the most personal information naturally receive the most access requests and are most predominantly represented in the number of access disputes brought to the attention of our office. In 2005-06, ICBC, the Vancouver Police Department and the Ministry of Public Safety and Solicitor General were the subject of more requests for review than other public bodies (see Table 3). The number of requests for review and complaints related to a public body is not necessarily a reflection of non-compliance.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

TABLE 3. DISPOSITION OF FIPPA REQUESTS FOR REVIEW, BY PUBLIC BODY

| | DISPOSITION | | | | | | |
|---|---|---|---|---|---|---|---|
| PUBLIC BODY | MEDIATED | NO REVIEWABLE ISSUE | NON JURISDICTIONAL | REFERRED TO PUBLIC BODY | WITHDRAWN | NOTICE OF INQUIRY ISSUED | TOTAL |
| Insurance Corporation of BC | 112 | 0 | 0 | 1 | 17 | 4 | 134 |
| Ministry of Public Safety and Solicitor General | 21 | 0 | 0 | 0 | 3 | 5 | 29 |
| Vancouver Police Department | 21 | 2 | 1 | 0 | 4 | 1 | 29 |
| Ministry of Attorney General | 21 | 0 | 1 | 0 | 2 | 4 | 28 |
| Ministry of Children and Family Development | 10 | 0 | 0 | 1 | 3 | 1 | 15 |
| Provincial Health Services Authority | 5 | 0 | 0 | 0 | 0 | 10 | 15 |
| Ministry of Health | 9 | 0 | 0 | 0 | 2 | 3 | 14 |
| Ministry of Employment and Income Assistance | 5 | 1 | 0 | 1 | 5 | 1 | 13 |
| Victoria Police Department | 8 | 0 | 0 | 0 | 3 | 0 | 11 |
| Vancouver Island Health Authority | 7 | 0 | 0 | 1 | 2 | 0 | 10 |
| All Other Public Bodies | 186 | 22 | 3 | 6 | 25 | 27 | 269 |
| **Total** | **405** | **25** | **5** | **9** | **66** | **56** | **566** |

Consistent with previous years, almost 81% of the requests for review filed with our office were from individuals. This is not surprising since the access process is a key mechanism for individuals who want to know what personal information government has about them or want to get copies of their own personal information from government.

Requests from the media accounted for 4% of the total number of requests for review, and the remaining 15% came from a wide variety of organizations and groups.

## Case Summaries: Requests for Review

### Losing Bidder Seeks Details of Winning Contract

After a health authority signed a food services contract, a competitor of the successful company asked to see the contract. The health authority released all except for three paragraphs dealing with purchasing, insurance and fiscal arrangements.

In withholding this information, the health authority cited section 21 of FIPPA, which requires the head of a public body to refuse to disclose information that might harm the business interests of a third party. Section 21 contains a three-part test, one part of which is that the information must be "supplied, implicitly or explicitly, in confidence". During our investigation, it became apparent that the content of the paragraphs in question had been negotiated rather than supplied, thus raising serious doubts about whether it could legitimately be withheld from the applicant.

The company providing the food services remained concerned that release of the information by the health authority could severely damage its ability to compete successfully for future contracts. Because of this, our Portfolio Officer initiated a three-way conference call with the health authority and the company, during which the latter agreed to the release of all remaining information save the annual payment for performing the contract. We advised the applicant of his right to ask the Commissioner to conduct an inquiry into whether the contract amount should be released as well, but he decided not to pursue the matter further.

### Litigation Privilege Applied to Vancouver Police Missing Women Review

A news reporter asked us to review the decision of the Vancouver Police Department to deny his request for a copy of the missing women investigation review completed by the Deputy Chief Constable.

The VPD took the position that the record was subject to what is commonly referred to as "litigation privilege", which is the legal privilege that applies to records or communications made for the conduct of litigation. The test for litigation privilege has two components. First, the record must have been created in reasonable contemplation of litigation. Second, the record must have been created for the dominant purpose of preparing for litigation.

With respect to the first branch of the test, the VPD provided copies of the two statements of claim registered by family members of missing women against the Vancouver Police Department and the City of Vancouver in April and September of 2002. The statements of claim established that litigation was reasonably contemplated at the time the record in dispute was created, as the investigation review was commenced shortly after the writs were filed.

With respect to the test of dominant purpose, we examined the review report itself, which specifically outlined the mandate and purpose of the review, and other documen-

Office of the Information & Privacy Commissioner for British Columbia

tation provided by the VPD that clearly established that legal counsel representing the VPD had requested that the VPD conduct a review of the response of the VPD to the complaints of missing women for the purpose of preparing for the civil litigation.

We gave our opinion to the applicant that the report was prepared in reasonable contemplation of litigation and for the dominant purpose of preparing for litigation and that, therefore, the record was covered by litigation privilege and was properly withheld by the VPD under section 14 of FIPPA. The applicant accepted our opinion.

**Access Denied to Non-existent Policies**

A woman asked a ministry for copies of the ministry's program's policies and procedures for dealing with parties submitting fraudulent claims. It seemed an innocuous request, so she was more than a little surprised to be told that disclosure was prohibited under a statutory provision that overrides the access provisions of FIPPA. She disagreed with this response on the grounds that the records she requested were not created pursuant to the other legislation and therefore were not subject to the override.

As a result of our mediation, the public body withdrew its reliance on the statutory provision. Instead, it announced that no records existed in response to scope of the applicant's request because there were no policies or procedures with respect to the submission of what the applicant described generally as "fraudulent claims". The public body did, however, give the applicant a written description of its general practices where claims were non-compliant. It also agreed to provide further information with respect to any specific issues that the applicant cared to identify. The applicant was satisfied with this offer and agreed to close the file.

**Woman Seeks Help Tracking Calls from Jails**

A woman who wanted to check whether she had received phone calls from correctional facilities asked for a list of all telephone numbers from three correctional facilities. The ministry withheld the list under section 15 of FIPPA on the ground that public disclosure of the telephone numbers could pose a threat to the security of the telephone system. Dissatisfied with this response, the woman asked our office to review it.

As a result of mediation, the applicant agreed to modify her request. She had made records of telephone numbers that had called her home phone, and was unfamiliar with some of them. With the agreement of the ministry, she provided our office with her list of numbers, which we then compared with lists the ministry provided of all telephone numbers of the three identified correctional facilities.

The comparison resulted in identifying two telephone numbers from one correctional facility and two numbers from another facility that appeared on the applicant's list. The applicant was satisfied and agreed to close the file.

**"Matter of Principle" Doesn't Stand Up as Reason for Withholding Records**

A woman who complained to a professional association about her treatment by various health professionals later asked the association for all records showing how it had dealt with her complaint. The association agreed to release responsive records with some severing of personal information and, as required by section 23 of FIPPA, asked the various health professionals if they had any concerns about the release of the severed records. All but one agreed to the release. The association disagreed with the health professional's reasons as to why the records should be withheld and said it would release the records unless the health professional requested a third-party review by our office.

Having received a request for review from the health professional, we reviewed the records and found that the information the association planned to release was not very sensitive personal information and almost all of it was known to the patient anyway. We discussed our review with the health professional, who admitted that his objection was based more on a "matter of principle" than on privacy concerns. After a detailed review of the records with us, the health professional agreed that the release of the records as severed by the association was a reasonable solution and withdrew his request for review. The severed records were released.

**Regional District Releases Environmental Report**

Responding to a request from an environmental foundation, a regional district denied access to an internal staff report. This report reviewed, from a scientific perspective, an Environment Canada study about the regional district's monitoring program at wastewater outfalls. The regional district withheld the report under section 13 of FIPPA as advice "developed by or for a public body".

The Portfolio Officer reviewed the report and found it to be a summary of expert comment on an issue of considerable concern to residents. The regional district feared that disclosure of such material would introduce a "chilling effect" to the free flow of ideas and communication within the public body.

The Portfolio Officer suggested that release of such a report would bring credit to the public body for professional work and contribute to the public understanding of an important issue.

It takes courage for a public body to do the right thing in a contentious situation. The regional district chose to release the report.

**Mayor's Appointment Reminders: Business or Personal?**

A journalist made a request for access to the appointment diary kept by the mayor of a municipality. The municipality responded to the request, severing some of the diary information under section 3(1)(i) of FIPPA, asserting that the record was "not in the

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

custody or control of the public body." The municipality argued that each entry in the diary constituted a separate record and that personal entries – which the municipality interpreted as including caucus meetings of a political organization – were not in its control.

We disagreed. The municipality revisited the matter and chose to release the previously severed entries, with the exception of those we agreed to be clearly personal (such as medical appointments and family events.). The matter was thus settled.

**Father's Hospital Records Could Hold Answers to Children's Health Risks**

A health authority turned down a request from an applicant for the hospital records of her deceased father. While acknowledging that the woman was her father's nearest relative, the health authority argued that the applicant wanted the records for her own interests rather than those of her father and thus was not entitled to exercise her father's rights under section 3(c) of the FIPPA Regulation. She disagreed, stating that she believed that the medical information about her father was important to determine if there were unknown health risks not only for herself but also for his other offspring.

During our discussions with the authority, it became apparent that its main concern was that the medical information was sufficiently complex that it might be misunderstood by a layperson, with potentially damaging results. The health authority offered to release the information to the family doctor of the applicant so that he could properly explain the records. The applicant agreed that this was a reasonable solution and the records were sent to the family doctor.

**Evidence Act Blocks Access to Committee Proceedings**

A woman who went to an emergency room with a detached retina later complained to the hospital about the quality of the treatment she received. Still dissatisfied after a review of her complaint by the health authority's quality assurance committee, she asked for copies of all records related to her emergency room visit. In response, the health authority fully disclosed the emergency room records but withheld all records related to the quality assurance committee's proceedings. She asked us to review that decision.

The health authority justified its decision on the basis that section 51 of the *Evidence Act* requires that records provided to a quality assurance committee or any resulting findings or conclusions of the committee not be disclosed in a legal proceeding or to anyone other than those listed in the section. Section 51 also specifically overrides any provisions of FIPPA. If section 51 applies, then FIPPA does not.

In order to determine if the health authority had properly applied the *Evidence Act* and met the criteria set out in section 51, we needed to review the contents of the

committee records and examine the policies and procedures describing the quality assurance process. The health authority provided documentation that demonstrated that the quality assurance committee was established for the purpose of improving medical care or medical practice in the hospital and that in general the committee met the criteria as set out in the *Evidence Act*. A review of the process used in this particular case demonstrated that the hospital followed its own procedures for streaming the applicant's concern to the quality assurance committee. Based on this information, we determined that section 51 of the *Evidence Act* applied, the health authority had withheld the records appropriately and FIPPA did not apply.

**Parent Asks for Hospital Records to Ensure Proper Care for Adult Son**

A woman made an access request for the health and psychiatric records related to the treatment at a hospital of her 20-year-old son. The public body denied access to the records on the grounds that the records contained sensitive personal information and that her son had refused to consent to their release.

His mother told us she considered the decision unreasonable because she and her husband were the life-long caregivers for their mentally ill child and needed access to the records in order to continue providing proper care. They believed that their son was not competent to make decisions about who should or should not have access to his personal information.

Section 3 of the FIPPA Regulation states that the right to access a record under FIPPA may be exercised by a parent or guardian if an individual is under the age of 19, by the individual's committee if the individual has a committee or by the individual's nearest relative or personal representative, if the individual is deceased.

As none of the conditions described by section 3 applied in this case, the public body was justified in withholding the records and indeed was obligated to do so. The applicant accepted this explanation.

**Wanted: Witness ID**

A Good Samaritan stopped to help a pedestrian who fell in a mall parking lot, then started to drive away once it appeared that she wasn't badly hurt. Thinking that it might be useful to have a witness to the accident, the pedestrian hastily recorded the licence plate number and description of the disappearing vehicle.

Later she called ICBC to find out how to contact the driver and was surprised to be told that ICBC wouldn't identify the vehicle owner to her because of privacy requirements. What if the accident resulted in a lawsuit? Surely her right to fair treatment trumped someone's right to privacy, she thought. She called our office to protest ICBC's decision.

Under section 22 of FIPPA, the head of a public body is required to refuse to disclose personal information to an applicant if the disclosure would be an unreasonable inva-

sion of a third party's personal privacy. After our office became involved, ICBC raised several arguments in support of its decision: the pedestrian might have recorded the licence plate number incorrectly; someone other than the registered owner might have been driving the vehicle; or the driver might not want to be involved further.

Had push come to shove, we would have been obliged to uphold ICBC's decision. Happily for the pedestrian, however, ICBC learned on further investigation that the registered owner of the vehicle was a company rather than an individual. As corporate contact information is not personal information, and is therefore not covered by section 22, ICBC agreed to provide the pedestrian with the name, address and telephone number of the company.

### Solicitor-Client Privilege Applies to Advice to Tribunals

A person who had lost his case in front of an administrative tribunal requested all records relating to his file. The administrative tribunal responded fully but withheld legal advice from a tribunal staff legal counsel on the basis that it was subject to solicitor-client privilege and therefore could be withheld under section 14 of FIPPA. The applicant argued that there is no solicitor-client relationship between the administrative tribunal staff lawyers and the tribunal members who decided his case.

We referred the applicant to previous decisions of the Commissioner in which he specifically confirmed that legal advice prepared by a tribunal's staff counsel for the tribunal is subject to solicitor-client privilege. The applicant accepted our opinion that the tribunal had properly withheld the records in dispute.

## Investigating and Resolving FIPPA Access Complaints

In addition to the right to request a review of a decision to sever or withhold information, people who have made access requests may file a complaint with the OIPC about the way the request was handled. If the dispute about an access request concerns a decision other than the decision to withhold or sever information, the matter is termed a "complaint."

Examples of complaint subjects include unreasonable access fees; delayed responses to access requests; inadequate searches for responsive records; and inappropriate time extensions. Although the 30 business day timeframe does not apply to complaints, a complaint should be filed at the earliest opportunity, since the OIPC may decline to investigate a complaint that has not been made in a timely fashion. Where a complainant has not already given the public body an opportunity to respond to and attempt to resolve the complaint, the OIPC will normally refer the complainant to the public body before the OIPC takes further action.

In 2005-06, the OIPC closed 260 complaints related to access requests, of which only five proceeded to a formal inquiry for resolution.

TABLE 4. DISPOSITION OF FIPPA ACCESS COMPLAINTS, BY TYPE

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TYPE | MEDIATED | NOT SUBSTANTIATED | PARTIALLY SUBSTANTIATED | SUBSTANTIATED | REFERRED TO PUBLIC BODY | NO REVIEWABLE ISSUE | WITHDRAWN | DECLINED TO INVESTIGATE | NOTICE OF INQUIRY ISSUED | TOTAL |
| Failure to fulfill any duty required by FIPPA (other than adequate search) | 35 | 30 | 7 | 17 | 37 | 10 | 9 | 7 | 1 | 153 |
| Unauthorized fees assessed (s.75) | 19 | 6 | 0 | 1 | 13 | 0 | 5 | 0 | 3 | 47 |
| Failure to conduct adequate search for records (s.6) | 9 | 14 | 0 | 2 | 17 | 0 | 2 | 0 | 1 | 45 |
| Unauthorized time extension taken by public body (s.10) | 4 | 4 | 3 | 1 | 2 | 0 | 1 | 0 | 0 | 15 |
| **Total** | **67** | **54** | **10** | **21** | **69** | **10** | **17** | **7** | **5** | **260** |

## Case Summaries: FIPPA Access Complaints

### Name Mix-up at MSP Triggers Records Search

A man who became aware of unusual activity in his Medical Services Plan file asked the Ministry of Health for a copy. It was later discovered that this activity (in the form of correspondence) had resulted from an administrative error involving another individual with the same name as the complainant. The ministry provided copies of records in response to the request, but the complainant believed that further records existed and, as proof, brought to the ministry's attention references in the released records to two documents that had not been included in the records released to him. He also asked for copies of any audiotapes of his telephone conversations with staff at MSP, as well as a key to decipher acronyms and other codes that appeared in the records released to him.

As a result of mediation, the ministry conducted a further search for the two records the complainant specified. It located and released one and provided a detailed description of its search for the other record. Although MSP staff had not recorded any of the complainant's telephone conversations, there were written notes pertaining to two of his calls and the ministry provided copies of the notes to him. MSP explained that it uses many codes on its database but does not have an up-to-date and comprehensive list of the codes. However, it identified a staff member who could assist the complainant in explaining any specific codes that he did not understand.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

### It Was All a Blur, Complainant Recalls

A man asked a police department for a copy of a photograph taken of him when he was arrested. The copy sent to him was of such a poor quality that he requested another, but the police department refused. He then complained to us that the department had not fulfilled its obligation under FIPPA.

The definition of "record" in FIPPA includes photographs and section 4 provides that a person who makes a request under the Act has a right of access to a record in the custody of a public body, including a record containing personal information about the applicant.

We did not have to decide if the police department's response had been adequate as the department, following a call from our investigator, adopted a more conciliatory approach and agreed to provide a better quality duplicate of the photograph.

### Legislative Gap Means Access Denied

Over the course of several requests for records, the applicant sought particular personnel information from the Greater Vancouver Transportation Authority (GVTA), more commonly known as Translink. The information sought in these requests related to employees of the British Columbia Rapid Transit Company, commonly known as Skytrain, and Coast Mountain Bus Company, which provides local bus service to Lower Mainland municipalities.

Translink had in the past responded openly and substantively to such requests in the belief that Skytrain and Coast Mountain, as operational divisions of Translink – a public body under FIPPA – were likewise subject to the disclosure provisions of FIPPA. Legal advice Translink received in the course of responding to one of the requests suggested otherwise. Translink therefore believed it had little choice but to decline to produce the requested records, on the ground that Skytrain and Coast Mountain were not public bodies covered by FIPPA.

Reviewing the particular section of FIPPA identified by legal counsel, we came to the same conclusion: the definition of "local government body" in FIPPA had been drafted and amended in such a way as to bring wholly-owned agencies and corporations under FIPPA, but not the subsidiaries of the GVTA. This was apparently because the GVTA had been added late to the list of local government bodies.

The Commissioner asked the ministry to correct this oversight. The ministry agreed and the ministry responsible for FIPPA made a ministerial order amending Schedule 2 to FIPPA, adding Skytrain and Coast Mountain to the list of public bodies.

## Investigating and Resolving FIPPA Privacy Complaints

Individuals who believe their personal information has been inappropriately collected, used or disclosed contrary to FIPPA may ask the Commissioner to investigate. As with

TABLE 5. DISPOSITION OF FIPPA PRIVACY COMPLAINTS, BY TYPE

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TYPE | MEDIATED | NOT SUBSTANTIATED | PARTIALLY SUBSTANTIATED | SUBSTANTIATED | REFERRED TO PUBLIC BODY | NO REVIEWABLE ISSUE | WITHDRAWN | DECLINED TO INVESTIGATE | NOTICE OF INQUIRY ISSUED | TOTAL |
| Unauthorized disclosure outside of the public body (s.33) | 7 | 16 | 2 | 0 | 20 | 1 | 4 | 1 | 1 | 52 |
| Unauthorized collection of information (ss.26&27) | 3 | 4 | 2 | 3 | 11 | 1 | 1 | 0 | 2 | 27 |
| Failure to correct information in a record (s.29) | 2 | 1 | 1 | 0 | 8 | 1 | 1 | 0 | 0 | 14 |
| Unauthorized use of information within a public body (s.32) | 2 | 2 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 5 |
| Failure to retain information for required timeline (s.31) | 0 | 0 | 0 | 0 | 1 | 2 | 1 | 0 | 0 | 4 |
| **Total** | **14** | **23** | **5** | **3** | **41** | **5** | **7** | **1** | **3** | **102** |

access complaints, where a person has not demonstrated that an attempt has been made to resolve a privacy complaint with the public body, the OIPC will generally refer the complainant to the public body for an attempt to resolve the matter at issue. If the complainant has done this and remains dissatisfied, the complainant may file a complaint with the OIPC, which will examine the matter and determine whether further investigation is warranted.

Privacy complaints are assigned to Portfolio Officers. They have delegated authority to investigate and resolve those complaints, either through mediation or by finding the complaint substantiated, unsubstantiated or partially substantiated. In this process, the Portfolio Officer examines all of the circumstances concerning the complaint, the legislation and relevant orders and discusses the matter with the complainant and the public body. If the complaint is determined to be wholly or partially substantiated, the Portfolio Officer will work with the public body to ensure that the problem is corrected or that steps have been taken to reduce the risk of a recurrence. Solutions may include changes in policies, procedures, training, technological fixes or a combination of any of these.

The OIPC closed 102 privacy complaints about public bodies in 2005-06.

TABLE 6. TYPES OF FIPPA ACCESS AND PRIVACY COMPLAINTS, BY PUBLIC BODY

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TYPE | ADEQUATE SEARCH | COLLECTION | CORRECTION | DISCLOSURE | OTHER DUTY REQUIRED BY ACT | FEES | RETENTION | TIME EXTENSION BY PUBLIC BODY | USE | TOTAL |
| Insurance Corporation of BC | 1 | 2 | 0 | 8 | 12 | 1 | 0 | 0 | 1 | 25 |
| Ministry of Public Safety and Solicitor General | 2 | 1 | 0 | 1 | 13 | 2 | 0 | 0 | 0 | 19 |
| Ministry of Children and Family Development | 3 | 0 | 2 | 5 | 7 | 0 | 0 | 0 | 0 | 17 |
| Ministry of Employment and Income Assistance | 1 | 1 | 1 | 3 | 10 | 0 | 1 | 0 | 0 | 17 |
| Vancouver Police Department | 1 | 2 | 2 | 1 | 8 | 3 | 0 | 0 | 0 | 17 |
| Ministry of Health | 5 | 3 | 0 | 2 | 4 | 2 | 0 | 0 | 0 | 16 |
| Ministry of Attorney General | 3 | 1 | 0 | 3 | 5 | 0 | 1 | 1 | 0 | 14 |
| WorkSafeBC | 2 | 1 | 0 | 5 | 5 | 0 | 0 | 0 | 1 | 14 |
| Vancouver Island Health Authority | 0 | 0 | 0 | 1 | 9 | 1 | 0 | 0 | 0 | 11 |
| Ministry of Finance | 1 | 0 | 0 | 0 | 4 | 4 | 0 | 1 | 0 | 10 |
| Translink | 1 | 0 | 0 | 0 | 4 | 0 | 0 | 5 | 0 | 10 |
| All Other Public Bodies | 25 | 16 | 9 | 23 | 72 | 34 | 2 | 8 | 3 | 192 |
| **Total** | **45** | **27** | **14** | **52** | **153** | **47** | **4** | **15** | **5** | **362** |

## Case Summaries: FIPPA Privacy Complaints

### Caller to Police Objects to Date-of-Birth Demand

A man who called a police department to report individuals ringing doorbells in the early morning hours was surprised to be asked his date of birth. When he hesitated to provide it, the complaint taker told him the information was necessary for his file and that if he did not provide it, the police department would get it by electronically accessing his driver's licence details.

The Chief Constable responded to this privacy complaint by telling the complainant that the department needs supplemental information in order to definitively identify persons providing information and had found date of birth, coupled with name, to be the most reliable identifier. The man asked our office whether such a demand complied with FIPPA's requirements regarding the collection of personal information by public bodies.

Responding to our investigation, the police department provided a more detailed explanation for its practice, saying that it is necessary to be able to identify individuals in case they contact the police department or the police department needs to contact them in future. The police department usually also collects further identifying information, such as home address and telephone number, for the same purpose. The department confirmed that it collects this information only for law enforcement purposes – one of the three purposes authorized by section 26 of FIPPA. However, when dealing with an individual who provides information to police but wishes to remain anonymous, the department will collect whatever information the individual provides without requiring precise identification. Finally, the department confirmed that accessing driver's licence information is not a common practice and takes place only where that information is necessary to assist an investigation.

The conclusion of the investigation was that the police department had demonstrated that it collected the date of birth from individuals providing law enforcement information for purposes in accordance with section 26(b) and (c) of FIPPA and the complaint was not substantiated. However, we pointed out that it would have been useful if the complaint taker had communicated the specific authority of police departments to collect personal information for law enforcement purposes and a better account of its information collection practices.

With a view to avoiding similar misunderstandings in future, we recommended that the police department reinforce with complaint takers the appropriate authority under FIPPA for collecting personal information about callers and how to deal with people who are reluctant to provide their personal information. The police department accepted this recommendation and the complainant was satisfied with the resolution of the complaint.

**School Bus Driver Objects to Video Surveillance**

Responding to safety concerns about student behaviour on a bus route, a school district installed video cameras on some buses to monitor behaviour and to assist the school district in case accusations were made by students against bus drivers. One of the drivers complained to us that the cameras weren't necessary on his bus and that he hadn't received a response from the school district to his concerns.

The school district was unable to provide documentation that the board had even discussed the issue or that it had passed a resolution authorizing video surveillance. Nor had the district developed any video surveillance policy or guidelines.

Section 26 of FIPPA states that no personal information may be collected by a public body unless another piece of provincial legislation authorizes the collection, the information is being collected for law enforcement purposes or the information being collected relates directly to and is necessary for an operating program of a public body.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

Since there was no other legislation authorizing the school district to collect personal information by video camera and the information was not being collected for law enforcement purposes, the only option available to the school district was to demonstrate that the video surveillance was directly related to and necessary to operate their bus program.

For the collection to be "necessary" in this case, the school district had to demonstrate that, without video surveillance, the school bus program (or a particular bus route) could not operate in a safe and efficient manner. Unable to make this case, the school district decided to halt the video surveillance program and to develop guidelines and policy to ensure compliance with FIPPA.

**Speak Your Mind at Public Hearings, But Prepare to Be Googled**

A woman made a submission to a public hearing convened by the municipality in which she lived. She later found that her name and address had been included in the meeting minutes posted to the municipality's website. Given the contentious nature of the issue being discussed at the public hearing, she was not happy with the publication of her address on the Internet. She complained to us about this apparent invasion of privacy by way of unauthorized disclosure.

In discussions with the municipality's webmaster, we learned that the municipality had agreed to remove the complainant's house number (but not street name) from the minutes. The municipality also provided some advice on how to remove information from popular Internet search engine Google's vast index – a procedure that does not work for all formats of electronic records.

We concluded that the municipality had done everything appropriate to assist the complainant in the circumstances. We also observed that accountability of public bodies is at the heart of FIPPA and, similarly, that the publication of minutes is a key part of local government accountability. Participants in public meetings traditionally have been required to provide evidence of their property ownership or place of residence in order to qualify as affected parties entitled to respond to particular development proposals. Long-standing practice aside, the municipality in this case agreed out of an abundance of caution to post conspicuous reminders to persons registering to speak at municipal meetings that their identity will be a matter of public record.

**The Primary Rule for Obtaining Consent: Get It in Writing**

A woman who was interviewed for a casual position with a school district was surprised to receive no notification of her success or failure to get the job. Finally she contacted the district office, only to be told that she had not been placed on the casual list because her references were unsatisfactory.

Curious about what had happened, she requested her file from the district and discovered that the interviewer had contacted individuals who were not on the list of

references she had provided. She complained to the district about this collection of her personal information without consent. Asked by the district to provide an explanation, the interviewer said that the additional reference had been discussed at the interview and that the woman had verbally provided consent during the interview to contact that reference. The woman denied this and complained to our office.

We investigated the complaint by interviewing the complainant and the employees of the district. The district had already investigated the matter and acknowledged that there were problems with the interview process. While it believed that its interviewer did have verbal authorization to contact the other reference, it realized that verbal consent was not sufficient to ensure that there were no misunderstandings between the district and prospective employees.

Following our investigation, the district decided to improve its reference check process by creating a consent form which an interviewee must sign if he or she agrees to any additional reference checks during the interview process. In addition, the district discussed the issue of reference checks at two meetings of the district school principals to ensure that all administrators were aware of their duties under FIPPA. The complainant was not completely satisfied with the outcome, as she believed she should be entitled to financial compensation. However, as the role of our office is remedial rather than punitive, we agreed that the district had taken appropriate steps to correct the problems.

**Personal Information on Hospital Admission Forms – How Much Is Too Much?**

A woman complained to us that hospital admitting staff had demanded too much personal information from her. She saw no good reason to justify the request for details about her citizenship, residency, religion, occupation and employer.

Section 26 of FIPPA limits the personal information a public body can collect from individuals. In the circumstance described by the complainant, a hospital can only collect personal information that is necessary to operate its programs in an effective and efficient manner.

Hospitals are responsible for making sure they know the identity of an admitted patient and that the patient qualifies to be a "beneficiary" of the Medical Services Plan or some other insurance plan. To determine if a patient meets residency requirements for MSP eligibility, the hospital has to ensure that the patient meets all three criteria for the definition of a resident as defined in the Medicare Protection Act – namely, that the patient is a citizen or is lawfully admitted to Canada for permanent residence, makes his or her home in BC and is physically present in BC at least six months in a calendar year.

Making this determination would require asking questions about an individual's citizenship, current address, length of residence at current address and previous addresses

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

if the individual has lived less than six months at their current address. Information about a patient's citizenship and residency status is necessary to ensure the hospital receives its funding from the Ministry of Health and the hospital is authorized by FIPPA to collect this information. It is not sufficient for a patient merely to provide a Care Card because hospitals don't have the means to electronically verify its validity.

Spiritual or pastoral care is an important element of good health for some people and is a legitimate program provided by hospitals. In this case, the admitting staff was simply asking the patient for her religion so that, if she subscribed to a religious belief, it could be noted on her chart. Under section 26 of FIPPA, hospitals are authorized to collect information that is related to and is necessary to operate a pastoral care program. However, hospitals must first determine if the patient wants to participate in such a program. Only when that question has been answered in the affirmative should hospital staff ask if the patient wants her or his religion noted on the chart.

It is not always necessary for a hospital to collect information about an individual's occupation or employer. If an individual presents a valid WorkSafe BC claim number, for example, a hospital would have no reason to collect additional information about the workplace. Where a workplace injury is presented and WorkSafe BC is not yet involved, it would be reasonable for the hospital to collect information about the accident, the employee's social insurance number and the employer's name, address and postal code because WorkSafe BC would likely be the insurer. If such a patient wants to make a WorkSafe BC claim, the hospital can simply provide a form to be filled out and forwarded to WorkSafe BC. If the reason for admitting has nothing to do with the workplace, there is no reason to collect information about an individual's occupation or employer.

The hospital agreed to review and change its information collection practices to comply with FIPPA requirements.

## Orders and Other Decisions

If a review or a complaint matter cannot be resolved through mediation, it may proceed to a formal inquiry. The mediation process is completely separate from the inquiry process. The Commissioner[5] has not been involved in nor is he privy to any of the discussions that occurred during the mediation phase. This is to ensure that, if the matter proceeds to an inquiry, the Commissioner is not perceived to be biased and can approach the matter with an open mind.

The Commissioner has the power to hold inquiries and decide all matters of law and fact and to dispose of the matter by issuing an order under section 58 of FIPPA. Inquiries can either be conducted in writing or in person. Most inquiries are conducted in writing.

At an inquiry, each party provides an initial submission outlining its perspective and

[5] References to the Commissioner include the Adjudicator as his delegate.

argument on the matter under review. Those submissions are exchanged between the parties and each party is given the right to reply. If the material in the submissions is confidential or sensitive, all or parts of that submission may be submitted in camera, which means that only the Commissioner will see that information.

At the end of an inquiry, the Commissioner will issue an order and the order becomes a public document. All orders are published on the OIPC website at www.oipc.bc.ca. Any order that deals with a matter concerning personal privacy is anonymized.

In making an order, the Commissioner has a number of options, including:

- requiring the public body to release more information;
- confirming the decision of the public body to withhold information;
- requiring the public body to refuse access to information;
- confirming, excusing or reducing a fee;
- requiring that a duty imposed by the Act be performed; and
- requiring a public body to stop collecting, using or disclosing information or to destroy information.

In 2005-06, we issued 32 FIPPA orders arising from 37 files (some orders dealt with more than one file). Of these 32 orders, 29 related to requests for review and the other three to complaints. Fourteen orders upheld the public body's decision, 7 overturned the public body's decision and the other 11 partially upheld the public body decision.

In addition, the Commissioner issued 10 other FIPPA decisions, principally about whether an inquiry would be held.

## Case Summaries: FIPPA Orders

Each of the orders summarized below can be read in full on our website.

### Order F05-20 – Ministry of Children and Family Development[4]

An adult adoptee requested records showing her birth father's name. In addition to stating the name of her birth mother (who, she said, had died a few months after her birth) and the names of her adoptive parents, she provided copies of her original registration of birth, her adoption order and her current identification.

The ministry provided the applicant with some records but refused access to the father's identifying information, on the basis that disclosure would unreasonably invade the privacy of third parties. The applicant said she had been told that, because her birth father was not named on her birth registration, she could not receive identifying information. She pointed out that her birth father had signed a paternity admission and also suggested that, since it was 60 years since her adoption, he was likely now dead. She argued that she was therefore entitled to have access to her birth father's identifying information.

[4] http://www.oipc.bc.ca/orders/2005/OrderF05-20.pdf

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

In the circumstances of this case, where paternity was not entirely certain and the wishes and views of the alleged father on disclosure of his identity were not known, the Adjudicator found that section 22 of FIPPA required the ministry to refuse disclosure of the third party's name to the applicant.

**Order F05-21 – Land and Water British Columbia Inc.[7]**

The applicant requested records related to a property. LWBC first responded by charging a fee of $1,140. Nine months later, after extensions and the expiry of the extended time lines, the matter proceeded to inquiry. LWBC disclosed the records in severed form during the inquiry process, waiving part of the fee. The applicant requested a refund of the deposit it had paid, as a remedy under section 58(3)(c) of FIPPA.

The Adjudicator found that LWBC had not shown that it had fulfilled its duties under sections 6(1) and 7 of FIPPA and, as a remedy under section 58(3)(c), ordered LWBC to refund the fees the applicant had paid.

**Order F05-24 – Abbotsford Police Department[8]**

The applicant sought access to records of a police investigation into a probable homicide of a young person. At the inquiry, the APD argued that, although the death occurred a number of years ago, the investigation was ongoing at the time of the request and the APD had not abandoned the possibility that the person it considered responsible for the death would be prosecuted. The APD therefore argued that, under sections 15(1)(a), 16(1)(b) and 22(3)(b) of FIPPA, it was entitled to refuse access to most of the records in the file. The Commissioner upheld the APD's decision to refuse access under these three exceptions.

**F05-26 – Forensic Psychiatric Services Commission[9]**

A patient in a hospital operated by the Commission requested his records from the Commission. The Commission replied that certain records are excluded from the scope of FIPPA under section 3(1)(h) because they "are related to a prosecution" and "all proceedings in respect of the prosecution have not been completed". The applicant was found to be not criminally responsible under Part XX.1 of the *Criminal Code* for certain crimes.

The Commissioner found that the applicant's prosecution ended with the verdict of not criminally responsible and the processes regarding his case under Part XX.1 are not proceedings in respect of the prosecution. The Commissioner therefore concluded that FIPPA applied to the records and ordered the Commission to process the applicant's request.

[7] http://www.oipc.bc.ca/orders/2005/OrderF05-21.pdf.
[8] http://www.oipc.bc.ca/orders/2005/OrderF05-24.pdf.
[9] http://www.oipc.bc.ca/orders/2005/OrderF05-26.pdf.

**Order F05-28 – Office of the Premier**[10]

The applicant sought records relating to development of the RAV line, a rail-based rapid transit line that will link central Richmond, Vancouver International Airport and Vancouver along the Cambie corridor to central Broadway, the downtown business district and Waterfront Station. The Office of the Premier disclosed some records and refused access to others under sections 12, 14, 16, 17, 21 and 22 of FIPPA.

The Commissioner confirmed that section 12(1) applied to records related to Treasury Board communications, discussions and decisions. The Commissioner also accepted that the financial and political issues involved in the conception and financial arrangements for the RAV project were, overall, of a sensitive and delicate nature and that section 16(1)(a) applied to other records. He also found that some information would, among other things, disclose negotiating positions of the Province and financial information relating to those negotiations and would interfere in a material way with the Province's ability to reach some or all of its objectives and that section 17(1)(e) therefore applied to that information.

Last, the Commissioner found that section 22(1) required the Office of the Premier to refuse disclosure of certain items, including an employee's home email address, that section 16(1)(b) applied to some information received in confidence from the federal government and that section 14 applied to records containing confidential communications between a lawyer and his client that were directly related to the seeking and giving of legal advice.

**Order F05-35 – City of Richmond**[11]

A City of Richmond employee made widely publicized allegations of harassment and other wrongdoing within the department in which the employee worked. The City retained a lawyer to investigate the employee's allegations of wrongdoing for the purpose of providing a fact-finding report and legal advice to the City. The lawyer found that the evidence did not support the allegations. A journalist requested a copy of the report, arguing that misinformation from the City about the lawyer's role negated the protection of legal professional privilege to the lawyer's report to the City.

The Commissioner found that on the face of the terms of reference signed by the City and the lawyer and the resulting report, the criteria for establishing legal professional privilege had been met and the report was privileged. He confirmed that the City was authorized by section 14 of FIPPA to refuse to disclose the report to the applicant journalist.

[10] http://www.oipc.bc.ca/orders/2005/OrderF05-28.pdf
[11] http://www.oipc.bc.ca/orders/2005/OrderF05-35.pdf

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

**Order F05-36 – Ministry of Agriculture and Lands (then Land and Water British Columbia Inc.)[12]**

An environmental group requested records related to the potential sale and development of Crown properties in the Shawnigan Lake area and asked for a waiver of the estimated $810 fee on public interest and financial grounds. Land and Water BC (LWBC) refused to waive the fee on both grounds.

After the applicant complained to the OIPC about the denial of the fee waiver, mediation led to a reduction of the fee to $220. LWBC continued to refuse to waive the fee and the matter proceeded to inquiry to consider LWBC's application of sections 75(a) and (b) of FIPPA.

The applicant, a small society with an interest in local water quality issues, showed from its bank statements that it could not afford the original or revised fee. Having considered LWBC's exercise of discretion, the Adjudicator found that a complete fee waiver was appropriate on the grounds that the applicant could not afford payment. The Adjudicator also found that a partial fee waiver was appropriate on public interest grounds, as some of the records related to environmental matters and that appropriate circumstances existed in which to waive the fee.

**Order F06-01 – Ministry of Energy, Mines and Petroleum Resources[13]**

The applicant requested access to records relating to a public report on offshore oil and gas exploration prepared for the Minister of Energy and Mines by a panel of three scientific experts. The ministry disclosed some records in its possession, subject to the exceptions in sections 12(1), 13(1) and 16(1) of FIPPA, and said that other information was not responsive to the request. It also said that, in light of "the contractual relationship with the third party who prepared all of the draft materials", records in the hands of the panel were not in the ministry's custody or under its control.

For records in the possession of the ministry, the Adjudicator found that section 12(1) applied to a small amount of information and sections 13(1) and 16(1) applied to some other information. The Adjudicator also found that some information in these records was incorrectly withheld as not responsive to the request but could be withheld under sections 13(1) and 16(1). Finally, the Adjudicator found that records in the possession of panel members or the panel secretariat were under the control of the ministry and subject to an access request under FIPPA. The Adjudicator ordered the ministry to process the request for the panel records.

[12] http://www.oipc.bc.ca/orders/2005/OrderF05-36.pdf
[13] http://www.oipc.bc.ca/orders/2006/OrderF06-01.pdf

# 4 THE YEAR IN REVIEW: PIPA FILES

## Investigating and Resolving PIPA Requests for Review and Complaints

The *Personal Information Protection Act* (PIPA) gives individuals the right to ask the OIPC to review matters where they are not satisfied with how an organization has

- responded to a request for personal information;
- responded to a request for correction of personal information;
- responded to a complaint about how it treats personal information; or
- followed or not followed any provision of PIPA.

A request for a review of an organization's decision, act or failure to act concerning a request for access to information or correction of personal information must be made to the OIPC within 30 business days after the organization's decision. A dispute concerning the collection, use and disclosure of personal information, fees or a dispute on any other matter is termed a "complaint". PIPA does not impose a time limit for making a complaint but, unless there are extenuating reasons, the OIPC will not generally entertain a complaint made more than six months after the individual concerned had notice of the circumstances.

The OIPC will generally defer or adjourn acting on a complaint or request for review until the individual concerned shows that he or she has communicated directly with the organization and enabled it to respond to or attempt to resolve the matter.

Our approach to PIPA requests for review and complaints is similar to the approach we take to FIPPA complaints. We investigate the circumstances of the dispute, consider the application of relevant sections of PIPA to those circumstances and, where practicable, involve the individual and the organization in efforts to arrive at a mediated resolution. Individuals or organizations that are dissatisfied with the results of mediation have the option of asking the Commissioner to conduct an inquiry.

In 2005-06, the OIPC received 47 requests for review and 134 complaints under PIPA and closed 49 requests for review and 146 complaints.

TABLE 7 DISPOSITION OF PIPA COMPLAINTS, BY TYPE

| | DISPOSITION | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| TYPE | MEDIATED | NOT SUBSTANTIATED | PARTIALLY SUBSTANTIATED | SUBSTANTIATED | REFERRED TO PUBLIC BODY | NO REVIEWABLE ISSUE | WITHDRAWN | DECLINED TO INVESTIGATE | NOTICE OF INQUIRY ISSUED | TOTAL |
| Failure to fulfill a duty required by PIPA (other than adequate search) | 17 | 5 | 1 | 2 | 15 | 5 | 2 | 3 | 4 | 54 |
| Inappropriate disclosure of personal information (s. 17) | 4 | 4 | 2 | 3 | 13 | 4 | 3 | 2 | 4 | 39 |
| Inappropriate collection of personal information (s. 11) | 1 | 8 | 2 | 2 | 11 | 2 | 2 | 0 | 2 | 30 |
| Failure to correct or annotate personal information when requested (s. 24) | 2 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 2 | 6 |
| Failure to conduct adequate search for records (s. 28) | 2 | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 5 |
| Unreasonable fees assessed (s.32) | 2 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 4 |
| Failure to retain personal information (s. 35) | 1 | 0 | 0 | 0 | 2 | 0 | 0 | 0 | 1 | 4 |
| Inappropriate use of personal information (s. 14) | 1 | 0 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 3 |
| Reprisal against employee (s.54) | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| **Total** | **30** | **18** | **5** | **9** | **46** | **12** | **7** | **5** | **14** | **146** |

TABLE 8 DISPOSITION OF PIPA REQUESTS FOR REVIEW, BY TYPE

| | DISPOSITION | | | | | | |
|---|---|---|---|---|---|---|---|
| PUBLIC BODY | MEDIATED | NO REVIEWABLE ISSUE | NON JURISDICTIONAL | REFERRED TO PUBLIC BODY | WITHDRAWN | NOTICE OF INQUIRY ISSUED | TOTAL |
| Failure to provide response to request for personal information (s. 28(b) | 15 | 7 | 1 | 7 | 3 | 0 | 33 |
| All personal information withheld from applicant (s.23) | 3 | 1 | 0 | 1 | 1 | 2 | 8 |
| Some personal information withheld from applicant (s.23) | 4 | 1 | 1 | 0 | 2 | 0 | 8 |
| **Total** | **22** | **9** | **2** | **8** | **6** | **2** | **49** |

## Case Summaries: PIPA Complaints

### Second Rule for Obtaining Consent – Get It If the Law Requires It

At a labour relations hearing, a former employer told a worker that he had contacted other previous employers to obtain personal information about the worker. The worker wrote to the former employer asking him what he had collected and for what purpose. The former employer did not fully respond and the worker asked us to investigate.

Our investigation revealed that the employer had contacted one other previous employer but had received no information. There was technically no breach of PIPA because no personal information had been collected or disclosed. However, we informed the former employer that he could not collect personal information about previous employees without their consent. PIPA describes circumstances in which an individual is deemed to consent to the collection of information (section 8) and in which personal information can be collected without consent (section 12), but the circumstance about which the worker complained did not fall into either category. (The "Guide for Businesses and Organizations to BC's PIPA"[14] and "PIPA and the Hiring Process"[15] on our website provide more information in this area.)

### Drawing the Line between Contact Information and Personal Information

A union local president complained that the executive of his union breached PIPA by disseminating emails containing his personal information to chairs and secretary-treasurers of the union without his consent.

We reviewed the emails in question and concluded that they did not contain the complainant's personal information. We concluded that, in the context of these emails, the complainant's email address and home telephone number were his con-

[14] http://www.oipc.bc.ca/pdfs/private/a-_GUIDE_TO_PIPA(3rd_ed).pdf

[15] http://www.oipc.bc.ca/pdfs/private/PIPAHiringFAQ(10APR06).pdf

tact information and were therefore excluded from the PIPA definition of "personal information".

**Club Protests Misuse of Membership List**

A private club complained that the trade union representing club members had used the club's membership list, which contained the names and telephone numbers of each of the club members, to compile a mailing list from which it sent two mailings to the club members to solicit their support in a labour dispute.

The trade union refused to respond to the club's questions about how it collected and used club members' personal information. However, after we reminded the trade union of its obligations under PIPA, it agreed to respond to the club's questions. It also agreed to purge the club membership information from its internal computer system and to ensure that all hard copies of the information were destroyed.

**Condo Owners at Odds Over Security Video System**

The strata council for a condominium development had received many complaints from residents about crime and vandalism, deteriorating levels of personal safety and a general decline in the livability of the development as a result of drug users, sex trade workers and petty criminals using parts of the building, its entrances and its covered parking. The council chose to have a security system installed at each of the entrances to the building and parking lot. The camera feeds were recorded to a computer hard drive in a locked utility room, which overwrote (records over) itself approximately every seven days. The live camera feeds were available to each resident (and only to residents) through a dedicated channel provided by the cable television supplier.

A number of residents were extremely unhappy about the recording of movements by residents and the live broadcast of these movements to other residents. They complained to the OIPC that the security system was collecting personal information without their consent, contrary to PIPA requirements.

In examining the matter, we found the complainants' allegations to be correct – their images were in fact being recorded and held over a rolling seven-day period and their images were being broadcast to building residents. At the same time, the strata council president argued that the overwhelming majority of residents endorsed the system and were grateful for the dramatic drop in vandalism, mischief and general intimidation since the system had been installed. In the final analysis, PIPA did not provide a solution to a situation where a majority of residents approved of the data collection and some did not. We wrote as follows:

> ...it would appear that a resolution of these concerns may be achieved with a measure of goodwill and continued discussion within the strata community at [address] as to how best to balance the benefits of the system with the perceived intrusiveness. For that, PIPA does not offer a definitive test other than that of "what a reasonable person would consider appropriate in the circumstances."

We closed the letter with a series of recommendations to the strata council concerning warning signage for the video surveillance system, developing a written policy and appointing a privacy officer and, at the strata corporation annual general meeting, revisiting the status of the system as an acceptable measure. We made a tentative finding of "partially substantiated" and advised that we could examine the issue again in the event of subsequent complaints.

**Housing Co-op Disclosures: Homeowner Grant Applicants**

People in housing co-operatives ("co-ops") are entitled to provincial homeowner grants, with additional grants being provided in the case of seniors, veterans and disabled persons. To get your grant, you fill out a form. In the case of co-ops, the Ministry of Small Business and Revenue provides one form ("Certificate of Eligible Occupants" or CEO) for the whole co-op complex, which may have several hundred units, each occupying one line of the form. Thus, signing the form for your unit may expose your personal information (unit number, name, birth date, phone number, disability status, assessed taxes based on value of unit, etc.) to other individuals.

A number of residents of a particular co-op complained that the CEO form was being taken door-to-door by a volunteer collecting the required signatures, with no provision for protecting the personal information of occupants – every signatory could see all the other information on the form. This was alleged to be contrary to the duty set out in section 34 of PIPA, to "make reasonable security arrangements to prevent unauthorized access."

In examining the issue, we found the complaint to be substantiated. In past years, the form had been covered by a sheet of cardboard from which a slot had been cut to enable the collection of a signature on the appropriate line without disclosing the personal information of others. We recommended that this practice be re-introduced and that, if possible, the required signatures be collected at the co-op office by a staff member or manager who could supervise the process to ensure privacy compliance. The co-op chose the latter option. Satisfied that this approach was compliant with the intent of PIPA, we considered the matter resolved.

**Housing Co-op Disclosures: Meeting Notices**

A member of a housing co-op ran afoul of other members following alleged misconduct on the premises by a family member. As a result, she faced an expulsion vote at a general meeting of the co-op membership. The co-op board posted a detailed notice of the pending vote meeting, and the reasons for it, in several public areas of the co-op property, including the recreation centre, which was accessible to guests of co-op members. The woman then complained to us that the quasi-public posting of information about her was contrary to PIPA and a defamatory invasion of her privacy,

especially since the matters that would be decided had not yet been the subject of the membership's vote.

PIPA section 18(o) permits the disclosure of a matter where "the disclosure is required or authorized by law". We found that the applicable law in this case, in addition to PIPA, was the *Cooperative Association Act*.

We found that the disclosure as effected by the board was permitted by PIPA section 18(o), but only to the extent that the disclosure is consistent with the law that requires or authorizes it. We recommended that the co-op board comply with PIPA by following its own rules and the *Cooperative Association Act*, requiring personal delivery of the notice to each member. Legal counsel for the co-op agreed and the practice of public posting of such notices stopped. On this basis, the complainant's concerns were resolved.

**Personal Information Pops Up in Ad**

A core purpose of privacy legislation is to prevent deliberate or unintentional misuse of personal information. Unfortunately, mistakes happen even with the best of intentions, with or without a sound privacy policy. One of our common roles is to mend fences where mistakes have been made.

A professional wanted to find a trusted person to come to her house every day and take care of her baby boy while she was at work. She put a notice in a community newspaper looking for just such a person. Soon afterwards she moved and sent the newspaper her updated contact information for its records.

The next week, when the woman opened the newspaper on the date the notice first appeared, she was appalled to see that the notice included her home address. When she contacted the newspaper to express her outrage, the office manager apologized profusely, explaining that the information had been put in the paper by mistake. The office manager said that the person who made the mistake had been reprimanded and offered to run the corrected ad free of charge for several weeks.

Although the error had been small, the impact on the advertiser was significant. Understandably, she continued to feel vulnerable and nervous. She felt that the paper hadn't gone far enough but she didn't want to have any further direct dealings with it. She asked us for assistance in arriving at a resolution to ensure that there was as little risk as possible from the notice having been run.

After we acted as an intermediary between the woman and the paper, the office manager provided assurance that the erroneous ad had been erased from the computer file and had been blocked out of archived issues. In addition, we gave the newspaper suggestions about useful resources for developing a privacy policy, including guidance on our website.[16]

[16] http://www.oipc.bc.ca/sector_private/resources/privacy_policy.htm

**The Agelessness of the Long-distance Runner**

The registration form for a popular 10-kilometre race asked participants to provide the day, month and year of their birth and their age in years as of the race day. One runner who objected was told that it wasn't mandatory information – if he was uncomfortable revealing his age he could put down a false age or, if he left the space blank, the organizers would randomly assign an age. He didn't think these were acceptable alternatives and complained to us that the organizers were asking for information they had no need to know.

PIPA provides that an organization may collect personal information only for purposes that a reasonable person would consider appropriate and must tell people why they are collecting their information. The run organizers told us that, after a race, they published the finish times and rankings, including placement within age and gender categories. They believed that many participants wanted this and noted that the conditions of entry on the run website stated that entrants were agreeing to publication, in any medium, of their name, gender and age category. The finishers' results were published in age bands such as 25-29, 30-34.

After considering the organizers' explanation and the requirements of PIPA, we found the complaint not to be substantiated. The run is a voluntary event and participants consent to the collection, use and disclosure of their personal information. The use to which it will be put is clearly described and appeared to be appropriate.

Even though we concluded that the race organizers had complied with PIPA, they expressed a willingness to consider, for future races, whether it might be feasible to create a zero age category or a registration system that would permit participants to identify only the age band into which they fall.

**Biometric Scan of Employees OK for Payroll Purposes in Some Circumstances...**

Demagnetization is a common failure of swipe cards used for monitoring actual time worked by employees. A hotel faced with this problem notified its employees that it would replace the swipe cards with a biometric scanning process. The process uses an image of an individual's finger to authenticate that the person who is entering or leaving the premises is that individual. It does not record the employee's fingerprint and therefore cannot later reproduce it. The system generates a number derived from measurements of various points of the subsurface of the employee's finger or thumb.

An employee brought his concerns to his manager and, when he felt his concerns were ignored, he requested our assistance. He said he considered the new system to be both an invasion of privacy and unnecessary, and argued that the employer hadn't explained why it was being implemented. He added he believed that requiring a thumbprint is invasive and wondered whether it was legal for the hotel to demand it, rather than providing an alternative option for employees to verify their identity and in and out times.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

PIPA authorizes the collection, use and disclosure of employee personal information without the consent of the individual employee, if it is "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual." We took the position that balancing an employee's right to protect his or her personal information against the authorization for the employer to use an employee's personal information without that employee's consent requires an employer to establish that

1. the sole purpose for the collection, use or disclosure of employee personal information is to establish, manage or terminate the employment relationship,
2. the purpose for the collection, use or disclosure of employee personal information is itself reasonable and
3. the collection, use or disclosure of employee personal information is reasonably required for that purpose.

In this case, the hotel established that it had until recently used signatures on paper for employee sign-in and -out. It had acquired an automated payroll system to produce more accurate payroll records. The system had a biometric capacity but, as an intermediate step, the hotel had used a swipe card alternative that proved unsatisfactory because of incompatibility with the hotel's door lock technology and problems with demagnetization. The finger scan was designed to verify the punch in and punch out times of employees in place of using swipe cards for that purpose.

The hotel confirmed that the finger scan system was being used only for the purpose of verifying employees' identity as a match to the number they punch in, to ensure accurate payroll and accurate records of which employees are in the building in case of emergencies. The hotel had previously had instances of employees using the wrong number to punch in and out and a general concern of some employees punching in and out for one another. The hotel agreed to give its employees more comprehensive notice of its intention to implement a biometric scanner as part of its new payroll system, and the complainant accepted our opinion that the hotel was authorized under PIPA to collect employee biometric information for payroll purposes.

### ... but Not OK in Others

Another hotel that was upgrading its payroll system was also considering the implementation of a hand scanning system to record employees' payroll punch-in and punch-out transactions using biometrics technology. It introduced the system on a trial basis without notifying the union representing the hotel's employees. The union filed a grievance alleging that "the hotel has violated ... the Personal Information Protection Act by implementing biometric hand scan system for time keeping which results in a search or physical examination of the employees' physical person and seizure of bodily

information without consent. The union believes this practice violates the employees' right to privacy in their physical integrity."

In this case, the hotel had informed the union that its primary purpose for implementing the hand scan technology with its new payroll system was to use the most advanced available technology to position itself "to be a leader in service, quality and technology." The hotel acknowledged to us that it "does not have a bona fide need to use the hand scan system from an employee relations perspective" and stated that the purpose of the hand scan system was not for monitoring employees. Under the hotel's lease arrangements with the payroll system provider, it could exchange the hand scan system for a card swipe system.

We were of the view that the hotel had failed to establish that the employee personal information collected by the hand scanner was reasonably required for the sole purpose of managing the employment relationship. Its stated purpose for implementing the hand scan technology was to use the most advanced available technology to position itself as an industry leader in technology. We considered that purpose to be related to marketing the hotel, rather than to establishing or managing the employment relationship with its employees.

The hotel accepted our opinion that it was not authorized under PIPA to collect employee biometric information in these circumstances. The hotel notified the union representing its employees that it would not be implementing the biometric component of its new payroll system.

## Case Summaries: PIPA Requests for Review

### A Lawyer Paid Is a Law File Earned

A client who has a parting of the ways with her lawyer and hires another should be able simply to pick up the file from the old office and deliver it to the new – unless she hasn't paid the bill. In that case, the unpaid lawyer might exercise what is called a "solicitor's lien" over the file materials, in which case the lawyer would hold the materials until the bill is paid.

A disaffected client who found his way to our office thought he had hit on a more imaginative way to get hold of his file: since the file materials contained his personal information and, since law offices are organizations subject to PIPA, the client requested a copy of his records under PIPA.

There was a slight problem: the information wasn't completely his. It was a matrimonial litigation file. The personal information of the client and his ex-spouse was so closely intertwined that to meet PIPA's requirements was next to impossible. PIPA makes it clear that a person may request his or her personal information from an organization, but not that of a "third party", meaning any other individual, such as the ex-spouse.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

Some information-access matters just weren't meant to be solved by PIPA. Fortunately, PIPA itself provides a way out: section 38(4) provides that the commissioner "may require an individual to attempt to resolve the individual's dispute with an organization in the way directed by the commissioner before the commissioner begins or continues a review or investigation under this Act of an applicant's complaint against the organization."

The Commissioner directed that the client avail himself of the appropriate remedies provided by sections 77 and 78 of the *Legal Profession Act*. On this basis, the file was closed.

**Worker Seeks Records Proving Workplace Injury**

A woman involved in a worker's compensation dispute with her former employer asked the company for certain information she felt would support her claim related to a carpal tunnel syndrome injury. She requested the name of the individual who had taken a photograph of her former workstation. She also asked for the names of former co-workers who had indicated to a manager that they remembered the applicant wearing a tensor bandage while at work.

The company responded by denying access to the identity of the photographer in accordance with section 23(4)(c) of PIPA. Moreover, it told her it had no record of the identities of the workers who had reported seeing the applicant wearing a tensor bandage at work.

PIPA gives applicants the right to request personal information only about themselves. It does not give them a right to request personal information about other individuals or general information about organizations. The name of the individual who took pictures of the applicant's former workstation is not the applicant's personal information. Therefore, PIPA did not require the company to disclose that information. The company confirmed that it had no record of the identities of the co-workers mentioned and no formal record of any statements that they may have made. The company, therefore, had no records responsive to this request and was in compliance with PIPA. The applicant accepted this assessment and agreed to close the file.

**Insurance Company Asks Doctor to Vet Medical File Before Release**

A woman asked her private medical insurance provider for a copy of her medical file. To ensure that there would be no harm in disclosing the entire contents of the file to her, the company gave it to her doctor instead and told her she could access his copy. She complained to us that the company had improperly disclosed the copy of the file to her physician. She wanted the physician to return the file to the company and the company to provide a copy directly to her.

As a result of mediation by our office, the company gave the complainant a complete copy of her file. The disclosure to the physician was found to be in compliance with section 23(4)(b) of PIPA and of section 5(1) of the regulations to PIPA, which permits organizations to disclose information relating to the mental or physical health of the individual to a health care professional, for the purpose of obtaining an assessment from the health care professional as to whether the disclosure of that information could reasonably be expected to result in grave and immediate harm to the individual's safety or mental or physical health. The physician determined that there would be no harm in disclosure and persuaded the complainant to agree to his retaining a copy of her file, as he had incorporated it into her personal medical file.

## Case Summaries: PIPA Orders

In 2005-06, the Commissioner issued four PIPA orders, of which three related to requests for a review and one to a complaint. The Commissioner also issued one decision related to a section 37 application to disregard an access request. Summaries of two orders follow:

### Order P05-01 – Collection of Personal Information by Canadian Tire[17]

A woman returning goods to a Canadian Tire store was asked to provide her name, address and telephone number but declined to do so. Instead she complained to us about the inappropriate collection of information by the organization operating the store.

At the inquiry, the Commissioner found that the organization's notices of purpose of collection complied with PIPA, although he encouraged the organization to improve them. The Commissioner also found that PIPA permitted the organization to require individuals to provide this personal information and to use it as part of its efforts to detect and deter fraudulent returns of goods. He concluded that this information was "necessary" for that purpose under section 7(2) of PIPA.

The Commissioner also said, however, that the organization could not require individuals to provide such personal information for the purpose of customer satisfaction follow-up, a purpose and use that must be made optional for customers. Finally, he found that section 35(2) of PIPA did not authorize the organization to retain personal information permanently, but he did not suggest a retention period.

### Order P06-01 – Access to Information in Dentist's Files[18]

The applicant requested access to her personal information in the hands of the organization, a dentist. The organization provided copies of the applicant's clinical records but refused access under sections 23(3)(a) and (c) and 23(4)(c) and (d) of PIPA to

[17] http://www.oipc.bc.ca/PIPAOrders/2005/OrderP05-01.pdf
[18] http://www.oipc.bc.ca/PIPAOrders/2006/OrderP06-01.pdf

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

its "College/Litigation file", comprising 16 records related to the applicant's complaint to the College of Dental Surgeons. The organization also said that it was not able to sever the records under section 23(5).

The Commissioner found that sections 23(4)(c) and (d) of PIPA did not apply to all of the information in the records and that severing under section 23(5) was possible. He also found, however, that the organization was authorized by section 23(3)(c) to refuse access to 15 records in their entirety and by section 23(3)(a) to refuse access to the sixteenth record.

# 5 THE YEAR IN REVIEW: OTHER OIPC ACTIVITIES

Most of the work of the OIPC is necessarily reactive. The bulk of the work that is done within the OIPC involves resolving complaints and appeals filed by citizens under both the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

However, a smaller but perhaps more critical role the OIPC plays is to comment proactively on any matter affecting access and privacy rights within and outside the province. The Commissioner has a role in relation to government and, to a certain extent, the private sector with respect to ensuring that new initiatives are appropriately restrained in the collection and use of personal information and to ensuring that the public's right of access is not diminished by new ways of doing business.

Under section 42 of FIPPA, the Commissioner has the authority to comment on how proposed policies, programs, legislation, data-matching schemes, automated information management systems and outsourcing arrangements impact on the access and privacy rights of BC citizens. The Commissioner has similar responsibilities under PIPA. Last year we updated our website to add information concerning the prevention of identity theft in order to assist businesses in protecting the personal information they have collected.

## Comments on Proposed Policy or Program Initiatives

In this general role, we commented on a number of initiatives in 2005-06, including this small but representative sample:

- a proposal for information sharing between the Vancouver School Board and the Vancouver Police Department, enabling the VPD to gain access to a database of student information on hand-held computers (the proposal did not proceed);
- a proposed municipal bylaw requiring bars to have video surveillance and ID scans;
- the Canadian Institute of Health Research's Canadian Longitudinal Study of Aging and the feasibility of accessing and linking provincial/territorial health care databases;
- a federal government proposal to merge the offices of the Information Commissioner of Canada and the Privacy Commissioner of Canada;
- a discussion paper on federal legislation to combat money laundering and terrorist financing;

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

- a federal government proposal to make it easier for law enforcement to gain access to internet data email communications;[19]
- the application of section 35(a.1) of FIPPA to certain research projects;
- the House of Commons Sub-Committee on Public Safety and National Security Review of the Anti-Terrorism Act;[20]
- the privacy implications of a student information software system shared by all participating public and independent schools and districts in BC;
- on-line posting of WorkSafe BC Incident Investigation Reports;
- a number of proposed municipal and school district video camera systems;
- a private sector organization's initiative to develop a PIPA policy to promote privacy awareness; and
- audit and compliance aspects of Police Records Information Management Environment of British Columbia (PRIME) a computer information system for municipal police forces and the RCMP in BC.

## Public Information Initiatives

Another important role of the OIPC is to inform the public, as well as public bodies and organizations, about their access and privacy rights and obligations under FIPPA and PIPA. These activities include keeping the OIPC's website current and easy to access; meeting with interest groups and stakeholders; participating as keynote speakers and panellists at conferences, seminars and other public forums; lecturing at colleges and universities; delivering training seminars; distributing informational materials; and engaging in dialogue with the media.

The following is a small sample of educational activities conducted by the Commissioner and OIPC staff in 2005-06:

**FIPPA:**

- BC Nurses Union meeting on the protection of personal information provided to the Union by its members;
- International Foundation workshops for Concepts and Practices of Canadian Benefits for Canadian and U.S. Corporations;
- 7th Annual Privacy & Security Conference;[21]
- Canadian Institute Cyber Security for Government Conference;[22]
- Canadian Bar Association Canadian Legal Conference and Expo 2005, [23]
- Financial Management Institute Public Sector Management Workshop 2005;
- Canadian Institute for the Administration of Justice Annual Conference;[24]

[19] http://www.oipc.bc.ca/pdfs/public/16763lawfulaccessltr(April8-2005).pdf
[20] http://www.oipc.bc.ca/pdfs/public/24915ATAreviewltr(April20-2005).pdf
[21] http://www.oipc.bc.ca/pdfs/Speeches/TransborderDataFlowsSpeech(10Feb06).pdf
[22] http://www.oipc.bc.ca/publications/speeches_presentations/CanInstCyberSecuritySpeech(Sept28-05).pdf
[23] http://www.oipc.bc.ca/pdfs/Speeches/CBA-AGMSpeech.pdf
[24] http://www.oipc.bc.ca/publications/speeches_presentations/CIAJSpeech(RevisedFinal)(Oct3-2005).pdf

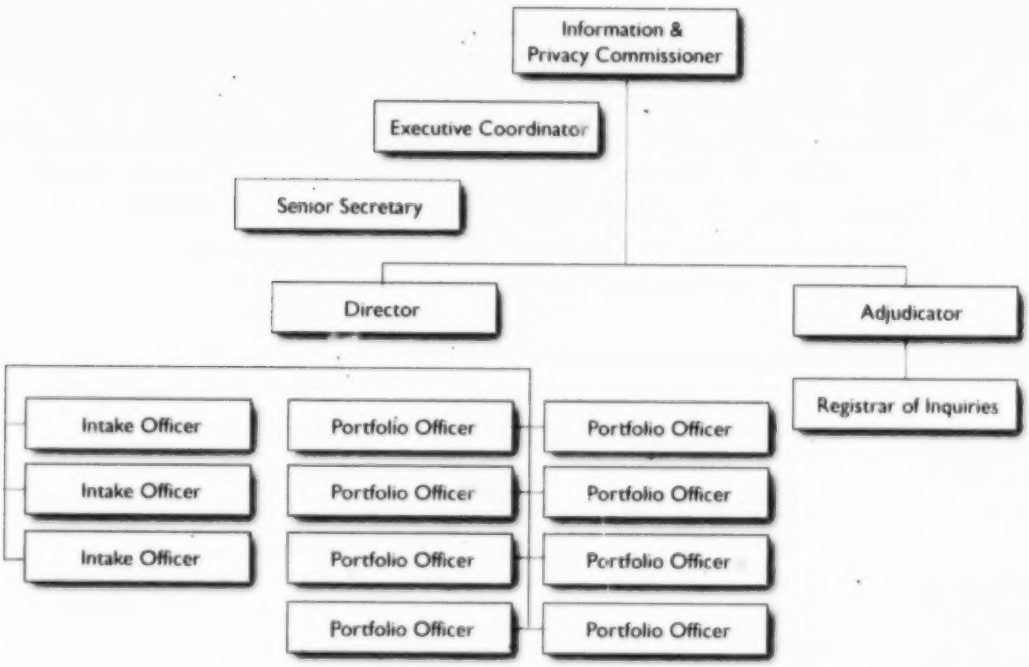
- MISA (organization for local government IT managers for BC);
- High Tech Crime Investigation Association;
- Canadian Association of Management Consultants meeting;
- Local Government Management Association Conference;
- FOI training for Esquimalt employees; and
- presentation to ICBC staff on "Top 10 things IT managers need to know about privacy"

**PIPA:**

- Vancity Group of Companies' Corporate Privacy Council and representatives from various departments and subsidiary organizations;
- Scam Jam 2006 (sponsored by the Better Business bureau of Vancouver);
- Business Council of BC's Annual Labour Relations Outlook session;
- Canadian Bar Association Labour & Employment Law Joint Section Meeting;
- BC Privacy Professionals Networking Forum;
- Law firm-sponsored session "Update on Employment Matters – Privacy: Recent Employment Related Decisions"; and
- Conference Board of Canada Council of Chief Privacy Officers

## ORGANIZATION CHART

The OIPC has 17 full time staff, including the Commissioner. It is a very lean organization, as the following chart demonstrates:



## FINANCIAL REPORTING

### 1. Authority

The Information and Privacy Commissioner is an independent officer of the legislature who monitors and enforces compliance with the *Freedom of Information and Protection of Privacy Act* and the *Personal Information Protection Act*. The *Freedom of Information and Protection of Privacy Act* applies to more than 2,200 public agencies and accords access to information and protection of privacy rights to citizens. The *Personal Information Protection Act* regulates the collection, use, access, disclosure and retention of personal information by more than 300,000 private sector organizations.

In addition, the Commissioner is the Registrar under the *Lobbyist Registration Act*, which requires those lobbying certain public agencies to register and pay a fee.

Funding for the operation of the Office of the Information and Privacy Commissioner is provided through a vote appropriation (Vote 5), as described below in note 3, and by recoveries for OIPC-run conferences. All OIPC payments are made from, and funds are deposited in, the Province's Consolidated Revenue Fund.

### 2. Significant Accounting Policies

These financial statements are prepared in accordance with generally accepted accounting principles in Canada. The significant accounting policies are as follows:

**a) Accrual basis**

The financial statements are accounted for on an accrual basis.

**b) Gross basis**

Revenue, including recoveries from government agencies, and expenses are recorded on a gross basis.

**c) Revenue**

Revenue is recognized when related costs are incurred.

**d) Expense**

Expense is recognized when goods and services are acquired or a liability is incurred.

**e) Net Assets**

The OIPC's net assets represent the accumulated cost of its capital assets less accumulated amortization.

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia

**f) Statement of Cash Flows**

A statement of cash flows has not been prepared as it would provide no additional useful information.

**g) Capital Assets**

Capital assets are recorded at cost less accumulated amortization. Amortization is provided on a straight-line basis over the estimated useful life of capital assets as follows:

| | |
|---|---|
| Computer hardware and software | 3 years |
| Furniture and equipment | 5 years |

## 3. Appropriations

Appropriations for the OIPC are approved by the Legislative Assembly of British Columbia and included in the government's budget estimates as voted through the *Supply Act*. The OIPC receives approval to spend funds through separate operating and capital appropriations. Any unused appropriations cannot be used by the OIPC in subsequent fiscal years and are returned to the Consolidated Revenue Fund.

| | 2006 (UNAUDITED) | | | 2005 (UNAUDITED) |
|---|---|---|---|---|
| | OPERATING | CAPITAL | TOTAL | TOTAL |
| Appropriations | $2,211,000 | $30,000 | $2,241,000 | $2,268,000 |
| Gross Funds Available | $2,211,000 | $30,000 | $2,241,000 | $2,268,000 |
| Operating Expenses | -$2,157,267 | 0 | -$2,157,267 | -$2,174,787 |
| Capital Acquisitions | 0 | -$3,413 | -$3,413 | -$12,419 |
| **Unused Appropriations** | **$53,733** | **$26,587** | **$80,320** | **$80,794** |

## 4. Employee Benefits and Leave Liability

Accumulated liability with respect to vacation and other leave entitlements due to employees of the OIPC amounted to $51,479 as at March 31, 2006. This liability is fully funded in the Leave Liability Account.

### 5. Capital Assets

| | 2006 (UNAUDITED) | | | 2005 (UNAUDITED) |
|---|---|---|---|---|
| | COST | ACCUMULATED AMORTIZATION | NET BOOK VALUE | ACCUMULATED AMORTIZATION |
| Computer Hardware and Software | $74,827 | -$54,421 | $20,406 | $32,915 |
| Furniture and Equipment | $3,582 | -$3,582 | $0 | $0 |
| **Total** | **$78,409** | **-$58,003** | **$20,406** | **$32,915** |

### 6. Commitments

The OIPC has a leasehold commitment with the British Columbia Buildings Corporation for building occupancy costs. Payments for office space for the fiscal 2006/07 are estimated at $126,996.00.

### 7. Pension and Retirement Benefits

The OIPC and its employees contribute to the Public Service Pension Plan ("Plan") in accordance with the *Public Sector Pension Plans Act*. The Plan is a multi-employer defined benefit plan and is available to substantially all of the OIPC's employees. On behalf of employers, the British Columbia Pension Corporation administers the Plan, including paying pension benefits to eligible employees. The most recent actuarial valuation (March 31, 2005) indicated that the pension fund had an unfunded liability. As a result, contribution rates were increased by 1.88% on April 1, 2006.

The OIPC also contributes, through the Province's payroll system, for specific termination benefits as provided for under collective agreements and conditions of employment for employees excluded from union membership. The cost of these employee future benefits is recognised in the year the contribution is paid.